

CompTIA

Exam Questions CAS-005

CompTIA SecurityX Exam



NEW QUESTION 1

An organization wants to implement a platform to better identify which specific assets are affected by a given vulnerability. Which of the following components provides the best foundation to achieve this goal?

- A. SASE
- B. CMDB
- C. SBOM
- D. SLM

Answer: B

Explanation:

A Configuration Management Database (CMDB) provides the best foundation for identifying which specific assets are affected by a given vulnerability. A CMDB maintains detailed information about the IT environment, including hardware, software, configurations, and relationships between assets. This comprehensive view allows organizations to quickly identify and address vulnerabilities affecting specific assets. References:

? CompTIA SecurityX Study Guide: Discusses the role of CMDBs in asset management and vulnerability identification.

? ITIL (Information Technology Infrastructure Library) Framework: Recommends the use of CMDBs for effective configuration and asset management.

? "Configuration Management Best Practices" by Bob Aiello and Leslie Sachs: Covers the importance of CMDBs in managing IT assets and addressing vulnerabilities.

NEW QUESTION 2

A security analyst is reviewing the following log:

Time	File type	Size	Antivirus status	Location
11:25	txt	25mb	block	c:\
11:27	dll	10mb	allow	c:\temp
11:29	doc	37mb	block	c:\users\user1\Desktop
11:32	pdf	13mb	allow	c:\users\user2\Downloads
11:35	txt	49mb	allow	c:\users\user3\Documents

Which of the following possible events should the security analyst investigate further?

- A. A macro that was prevented from running
- B. A text file containing passwords that were leaked
- C. A malicious file that was run in this environment
- D. A PDF that exposed sensitive information improperly

Answer: B

Explanation:

Based on the log provided, the most concerning event that should be investigated further is the presence of a text file containing passwords that were leaked. Here's why:

? Sensitive Information Exposure: A text file containing passwords represents a significant security risk, as it indicates that sensitive credentials have been exposed in plain text, potentially leading to unauthorized access.

? Immediate Threat: Password leaks can lead to immediate exploitation by attackers, compromising user accounts and sensitive data. This requires urgent investi

NEW QUESTION 3

Users must accept the terms presented in a captive portal when connecting to a guest network. Recently, users have reported that they are unable to access the Internet after joining the network A network engineer observes the following:

- Users should be redirected to the captive portal.
- The Motive portal runs TL. S 1 2
- Newer browser versions encounter security errors that cannot be bypassed
- Certain websites cause unexpected re directs

Which of the following now likely explains this behavior?

- A. The TLS ciphers supported by the captive portal ate deprecated
- B. Employment of the HSTS setting is proliferating rapidly.
- C. Allowed traffic rules are causing the NIPS to drop legitimate traffic
- D. An attacker is redirecting supplicants to an evil twin WLAN.

Answer: A

Explanation:

The most likely explanation for the issues encountered with the captive portal is that the TLS ciphers supported by the captive portal are deprecated. Here??s why:

? TLS Cipher Suites: Modern browsers are continuously updated to support the latest security standards and often drop support for deprecated and insecure cipher suites. If the captive portal uses outdated TLS ciphers, newer browsers may refuse to connect, causing security errors.

? HSTS and Browser Security: Browsers with HTTP Strict Transport Security (HSTS) enabled will not allow connections to sites with weak security configurations. Deprecated TLS ciphers would cause these browsers to block the connection.

? References:

By updating the TLS ciphers to modern, supported ones, the security engineer can ensure compatibility with newer browser versions and resolve the connectivity issues reported by users.

NEW QUESTION 4

A user submits a help desk ticket stating their account does not authenticate sometimes. An analyst reviews the following logs for the user:
Which of the following best explains the reason the user's access is being denied?

- A. incorrectly typed password
- B. Time-based access restrictions
- C. Account compromise
- D. Invalid user-to-device bindings

Answer: B

Explanation:

The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non-business hours, reducing the risk of security incidents.

References:

? CompTIA SecurityX Study Guide: Covers various access control methods, including time-based restrictions, as a means of enhancing security.

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends the use of time-based access restrictions as part of access control policies.

? "Access Control and Identity Management" by Mike Chapple and Aaron French: Discusses the implementation and benefits of time-based access restrictions.

NEW QUESTION 5

A security engineer is developing a solution to meet the following requirements?

- All endpoints should be able to establish telemetry with a SIEM.
- All endpoints should be able to be integrated into the XDR platform.
- SOC services should be able to monitor the XDR platform

Which of the following should the security engineer implement to meet the requirements?

- A. CDR and central logging
- B. HIDS and vTPM
- C. WAF and syslog
- D. HIPS and host-based firewall

Answer: D

Explanation:

To meet the requirements of having all endpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host-based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.

References:

? CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms.

? NIST Special Publication 800-94, "Guide to Intrusion Detection and Prevention Systems (IDPS)": Highlights the capabilities of HIPS for security monitoring and incident response.

? "Network Security Monitoring" by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

NEW QUESTION 6

Recent reports indicate that a software tool is being exploited. Attackers were able to bypass user access controls and load a database. A security analyst needs to find the vulnerability and recommend a mitigation. The analyst generates the following output:

```
C:\>whoami
local-user
C:\>netuser local-user Welcome!
The command completed successfully!
C:\>dbloader.exe local-user Welcome!
Insufficient Permissions. Now Closing...
C:\>strings dbloader.exe
!This program cannot be run in DOS Mode
dB10ad3r!
Load Database jmp
182(*nx
(i3jN*jk
fahn82mk0a
C:\>dbloader.exe admin dB10ad3r!
```

Which of the following would the analyst most likely recommend?

- A. Installing appropriate EDR tools to block pass-the-hash attempts
- B. Adding additional time to software development to perform fuzz testing

- C. Removing hard coded credentials from the source code
- D. Not allowing users to change their local passwords

Answer: C

Explanation:

The output indicates that the software tool contains hard-coded credentials, which attackers can exploit to bypass user access controls and load the database. The most likely recommendation is to remove hard-coded credentials from the source code. Here??s why:

- ? Security Best Practices: Hard-coded credentials are a significant security risk because they can be easily discovered through reverse engineering or simple inspection of the code. Removing them reduces the risk of unauthorized access.
- ? Credential Management: Credentials should be managed securely using environment variables, secure vaults, or configuration management tools that provide encryption and access controls.
- ? Mitigation of Exploits: By eliminating hard-coded credentials, the organization can prevent attackers from easily bypassing authentication mechanisms and gaining unauthorized access to sensitive systems.
- ? References:

NEW QUESTION 7

A security analyst is reviewing the following authentication logs:

Date	Time	Computer	Account	Log-in success?
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM08	User8	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM01	User1	No
12/15	8:01:23AM	VM12	User12	Yes
12/15	8:01:23AM	VM01	User1	Yes
12/15	8:01:23AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:24AM	VM01	User2	No
12/15	8:01:25AM	VM01	User2	No
12/15	8:01:25AM	VM08	User8	Yes

Which of the following should the analyst do first?

- A. Disable User2's account
- B. Disable User12's account
- C. Disable User8's account
- D. Disable User1's account

Answer: D

Explanation:

Based on the provided authentication logs, we observe that User1's account experienced multiple failed login attempts within a very short time span (at 8:01:23 AM on 12/15). This pattern indicates a potential brute-force attack or an attempt to gain unauthorized access. Here??s a breakdown of why disabling User1's account is the appropriate first step:

- ? Failed Login Attempts: The logs show that User1 had four consecutive failed login attempts:
- ? Security Protocols and Best Practices: According to CompTIA Security+ guidelines, multiple failed login attempts within a short timeframe should trigger an immediate response to prevent further potential unauthorized access attempts. This typically involves temporarily disabling the account to stop ongoing brute-force attacks.
- ? Account Lockout Policy: Implementing an account lockout policy is a standard practice to thwart brute-force attacks. Disabling User1's account will align with these best practices and prevent further failed attempts, which might lead to successful unauthorized access if not addressed.
- ? References:

By addressing User1's account first, we effectively mitigate the immediate threat of a brute- force attack, ensuring that further investigation can be conducted without the risk of unauthorized access continuing during the investigation period.

NEW QUESTION 8

An organization is looking for gaps in its detection capabilities based on the APTs that may target the industry Which of the following should the security analyst use to perform threat modeling?

- A. ATT&CK

- B. OWASP
- C. CAPEC
- D. STRIDE

Answer: A

Explanation:

The ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is the best tool for a security analyst to use for threat modeling when looking for gaps in detection capabilities based on Advanced Persistent Threats (APTs) that may target the industry. Here's why:

? Comprehensive Framework: ATT&CK provides a detailed and structured repository of known adversary tactics and techniques based on real-world observations. It helps organizations understand how attackers operate and what techniques they might use.

? Gap Analysis: By mapping existing security controls against the ATT&CK matrix, analysts can identify which tactics and techniques are not adequately covered by current detection and mitigation measures.

? Industry Relevance: The ATT&CK framework is continuously updated with the latest threat intelligence, making it highly relevant for industries facing APT threats. It provides insights into specific APT groups and their preferred methods of attack.

? References:

NEW QUESTION 9

Which of the following AI concerns is most adequately addressed by input sanitation?

- A. Model inversion
- B. Prompt Injection
- C. Data poisoning
- D. Non-explainable model

Answer: B

Explanation:

Input sanitation is a critical process in cybersecurity that involves validating and cleaning data provided by users to prevent malicious inputs from causing harm. In the context of AI concerns:

? A. Model inversion involves an attacker inferring sensitive data from model outputs, typically requiring sophisticated methods beyond just manipulating input data.

? B. Prompt Injection is a form of attack where an adversary provides malicious input to manipulate the behavior of AI models, particularly those dealing with natural language processing (NLP). Input sanitation directly addresses this by ensuring that inputs are cleaned and validated to remove potentially harmful commands or instructions that could alter the AI's behavior.

? C. Data poisoning involves injecting malicious data into the training set to compromise the model. While input sanitation can help by filtering out bad data, data poisoning is typically addressed through robust data validation and monitoring during the model training phase, rather than real-time input sanitation.

? D. Non-explainable model refers to the lack of transparency in how AI models make decisions. This concern is not addressed by input sanitation, as it relates more to model design and interpretability techniques.

Input sanitation is most relevant and effective for preventing Prompt Injection attacks, where the integrity of user inputs directly impacts the performance and security of AI models.

References:

? CompTIA Security+ Study Guide

? "Security of Machine Learning" by Battista Biggio, Blaine Nelson, and Pavel Laskov

? OWASP (Open Web Application Security Project) guidelines on input validation and injection attacks

Top of Form Bottom of Form

NEW QUESTION 10

Company A and Company D ate merging Company A's compliance reports indicate branch protections are not in place A security analyst needs to ensure that potential threats to the software development life cycle are addressed. Which of the following should me analyst cons<der when completing this basic?

- A. If developers are unable to promote to production
- B. If DAST code is being stored to a single code repository
- C. If DAST scans are routinely scheduled
- D. If role-based training is deployed

Answer: C

Explanation:

Dynamic Application Security Testing (DAST) is crucial for identifying and addressing security vulnerabilities during the software development life cycle (SDLC). Ensuring that DAST scans are routinely scheduled helps in maintaining a secure development process. Why Routine DAST Scans?

? Continuous Security Assessment: Regular DAST scans help in identifying vulnerabilities in real-time, ensuring they are addressed promptly.

? Compliance: Routine scans ensure that the development process complies with security standards and regulations.

? Proactive Threat Mitigation: Regular scans help in early detection and mitigation of potential security threats, reducing the risk of breaches.

? Integration into SDLC: Ensures security is embedded within the development process, promoting a security-first approach.

Other options, while relevant, do not directly address the continuous assessment and proactive identification of threats:

? A. If developers are unable to promote to production: This is more of an operational issue than a security assessment.

? B. If DAST code is being stored to a single code repository: This concerns code management rather than security testing frequency.

? D. If role-based training is deployed: While important, training alone does not ensure continuous security assessment.

References:

? CompTIA SecurityX Study Guide

? OWASP Testing Guide

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations"

NEW QUESTION 10

A security engineer is given the following requirements:

- An endpoint must only execute Internally signed applications
 - Administrator accounts cannot install unauthorized software.
 - Attempts to run unauthorized software must be logged Which of the following best meets these requirements?
- A. Maintaining appropriate account access through directory management and controls
B. Implementing a CSPM platform to monitor updates being pushed to applications
C. Deploying an EDR solution to monitor and respond to software installation attempts
D. Configuring application control with blocked hashes and enterprise-trusted root certificates

Answer: D

Explanation:

To meet the requirements of only allowing internally signed applications, preventing unauthorized software installations, and logging attempts to run unauthorized software, configuring application control with blocked hashes and enterprise-trusted root certificates is the best solution. This approach ensures that only applications signed by trusted certificates are allowed to execute, while all other attempts are blocked and logged. It effectively prevents unauthorized software installations by restricting execution to pre- approved applications.

References:

? CompTIA SecurityX Study Guide: Describes application control mechanisms and the use of trusted certificates to enforce security policies.

? NIST Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations": Recommends application whitelisting and execution control for securing endpoints.

? "The Application Security Handbook" by Mark Dowd, John McDonald, and Justin Schuh: Covers best practices for implementing application control and managing trusted certificates

NEW QUESTION 13

A security analyst reviews the following report:

	Location	Chassis manufacturer	OS	Application developer	Vendor
Product A	United States	Local company A	Debian 11	Unknown	Charlie Security Consulting
Product B	United States	Global company B	Red Hat Enterprise Linux	Developer B	BigBox Vulnerabilities

Which of the following assessments is the analyst performing?

- A. System
B. Supply chain
C. Quantitative
D. Organizational

Answer: B

Explanation:

The table shows detailed information about products, including location, chassis manufacturer, OS, application developer, and vendor. This type of information is typically assessed in a supply chain assessment to evaluate the security and reliability of components and services from different suppliers.

Why Supply Chain Assessment?

? Component Evaluation: Assessing the origin and security of each component used in the products, including hardware, software, and third-party services.

? Vendor Reliability: Evaluating the security practices and reliability of vendors involved in providing components or services.

? Risk Management: Identifying potential risks associated with the supply chain, such as vulnerabilities in third-party components or insecure development practices.

Other types of assessments do not align with the detailed supplier and component information provided:

? A. System: Focuses on individual system security, not the broader supply chain.

? C. Quantitative: Focuses on numerical risk assessments, not supplier information.

? D. Organizational: Focuses on internal organizational practices, not external suppliers.

References:

? CompTIA SecurityX Study Guide

? NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"

? "Supply Chain Security Best Practices," Gartner Research

NEW QUESTION 15

A company receives reports about misconfigurations and vulnerabilities in a third-party hardware device that is part of its released products. Which of the following solutions is the best way for the company to identify possible issues at an earlier stage?

- A. Performing vulnerability tests on each device delivered by the providers
B. Performing regular red-team exercises on the vendor production line
C. Implementing a monitoring process for the integration between the application and the vendor appliance
D. Implementing a proper supply chain risk management program

Answer: D

Explanation:

Addressing misconfigurations and vulnerabilities in third-party hardware requires a comprehensive approach to manage risks throughout the supply chain. Implementing a proper supply chain risk management (SCRM) program is the most effective solution as it encompasses the following:

? Holistic Approach: SCRM considers the entire lifecycle of the product, from initial design through to delivery and deployment. This ensures that risks are identified and managed at every stage.

? Vendor Management: It includes thorough vetting of suppliers and ongoing

assessments of their security practices, which can identify and mitigate vulnerabilities early.

? Regular Audits and Assessments: A robust SCRM program involves regular audits

and assessments, both internally and with suppliers, to ensure compliance with security standards and best practices.

? Collaboration and Communication: Ensures that there is effective communication

and collaboration between the company and its suppliers, leading to faster identification and resolution of issues.

Other options, while beneficial, do not provide the same comprehensive risk management:

? A. Performing vulnerability tests on each device delivered by the providers: While useful, this is reactive and only addresses issues after they have been delivered.

? B. Performing regular red-team exercises on the vendor production line: This can identify vulnerabilities but is not as comprehensive as a full SCRM program.

? C. Implementing a monitoring process for the integration between the application and the vendor appliance: This is important but only covers the integration phase, not the entire supply chain.

References:

? CompTIA SecurityX Study Guide

? NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"

? ISO/IEC 27036-1:2014, "Information technology — Security techniques — Information security for supplier relationships"

NEW QUESTION 19

A financial technology firm works collaboratively with business partners in the industry to share threat intelligence within a central platform This collaboration gives partner organizations the ability to obtain and share data associated with emerging threats from a variety of adversaries Which of the following should the organization most likely leverage to facilitate this activity? (Select two).

A. CWPP

B. YAKA

C. ATTACK

D. STIX

E. TAXII

F. JTAG

Answer: DE

Explanation:

? D. STIX (Structured Threat Information eXpression): STIX is a standardized language for representing threat information in a structured and machine-readable format. It facilitates the sharing of threat intelligence by ensuring that data is consistent and can be easily understood by all parties involved.

? E. TAXII (Trusted Automated eXchange of Indicator Information): TAXII is a transport mechanism that enables the sharing of cyber threat information over a secure and trusted network. It works in conjunction with STIX to automate the exchange of threat intelligence among organizations.

Other options:

? A. CWPP (Cloud Workload Protection Platform): This focuses on securing cloud workloads and is not directly related to threat intelligence sharing.

? B. YARA: YARA is used for malware research and identifying patterns in files, but it is not a platform for sharing threat intelligence.

? C. ATT&CK: This is a knowledge base of adversary tactics and techniques but does not facilitate the sharing of threat intelligence data.

? F. JTAG: JTAG is a standard for testing and debugging integrated circuits, not related to threat intelligence.

References:

? CompTIA Security+ Study Guide

? "STIX and TAXII: The Backbone of Threat Intelligence Sharing" by MITRE

? NIST SP 800-150, "Guide to Cyber Threat Information Sharing"

NEW QUESTION 23

A company wants to invest in research capabilities with the goal to operationalize the research output. Which of the following is the best option for a security architect to recommend?

A. Dark web monitoring

B. Threat intelligence platform

C. Honeypots

D. Continuous adversary emulation

Answer: B

Explanation:

Investing in a threat intelligence platform is the best option for a company looking to operationalize research output. A threat intelligence platform helps in collecting, processing, and analyzing threat data to provide actionable insights. These platforms integrate data from various sources, including dark web monitoring, honeypots, and other security tools, to offer a comprehensive view of the threat landscape.

Why a Threat Intelligence Platform?

? Data Integration: It consolidates data from multiple sources, including dark web monitoring and honeypots, making it easier to analyze and derive actionable insights.

? Actionable Insights: Provides real-time alerts and reports on potential threats, helping the organization take proactive measures.

? Operational Efficiency: Streamlines the process of threat detection and response, allowing the security team to focus on critical issues.

? Research and Development: Facilitates the operationalization of research output by providing a platform for continuous monitoring and analysis of emerging threats.

Other options, while valuable, do not offer the same level of integration and operationalization capabilities:

? A. Dark web monitoring: Useful for specific threat intelligence but lacks comprehensive operationalization.

? C. Honeypots: Effective for detecting and analyzing specific attack vectors but not for broader threat intelligence.

? D. Continuous adversary emulation: Important for testing defenses but not for integrating and operationalizing threat intelligence.

References:

? CompTIA SecurityX Study Guide

? "Threat Intelligence Platforms," Gartner Research

? NIST Special Publication 800-150, "Guide to Cyber Threat Information Sharing"

NEW QUESTION 25

A company wants to install a three-tier approach to separate the web. database, and application servers A security administrator must harden the environment which of the following is the best solution?

- A. Deploying a VPN to prevent remote locations from accessing server VLANs
- B. Configuring a SASb solution to restrict users to server communication
- C. Implementing microsegmentation on the server VLANs
- D. installing a firewall and making it the network core

Answer: C

Explanation:

The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs. Here??s why:

- ? Enhanced Security: Microsegmentation creates granular security zones within the data center, allowing for more precise control over east-west traffic between servers. This helps prevent lateral movement by attackers who may gain access to one part of the network.
- ? Isolation of Tiers: By segmenting the web, database, and application servers, the organization can apply specific security policies and controls to each segment, reducing the risk of cross-tier attacks.
- ? Compliance and Best Practices: Microsegmentation aligns with best practices for network security and helps meet compliance requirements by ensuring that sensitive data and systems are properly isolated and protected.
- ? References:

NEW QUESTION 29

Third parties notified a company's security team about vulnerabilities in the company's application. The security team determined these vulnerabilities were previously disclosed in third-party libraries. Which of the following solutions best addresses the reported vulnerabilities?

- A. Using IaC to include the newest dependencies
- B. Creating a bug bounty program
- C. Implementing a continuous security assessment program
- D. Integrating a SASI tool as part of the pipeline

Answer: D

Explanation:

The best solution to address reported vulnerabilities in third-party libraries is integrating a Static Application Security Testing (SAST) tool as part of the development pipeline. Here??s why:

- ? Early Detection: SAST tools analyze source code for vulnerabilities before the code is compiled. This allows developers to identify and fix security issues early in the development process.
- ? Continuous Security: By integrating SAST tools into the CI/CD pipeline, the organization ensures continuous security assessment of the codebase, including third-party libraries, with each code commit and build.
- ? Comprehensive Analysis: SAST tools provide a detailed analysis of the code, identifying potential vulnerabilities in both proprietary code and third-party dependencies, ensuring that known issues in libraries are addressed promptly.
- ? References:

NEW QUESTION 30

A financial services organization is using AI to fully automate the process of deciding client loan rates. Which of the following should the organization be most concerned about from a privacy perspective?

- A. Model explainability
- B. Credential Theft
- C. Possible prompt injections
- D. Exposure to social engineering

Answer: A

Explanation:

When using AI to fully automate the process of deciding client loan rates, the primary concern from a privacy perspective is model explainability.

Why Model Explainability is Critical:

- ? Transparency: It ensures that the decision-making process of the AI model can be understood and explained to stakeholders, including clients.
- ? Accountability: Helps in identifying biases and errors in the model, ensuring that the AI is making fair and unbiased decisions.
- ? Regulatory Compliance: Various regulations require that decisions, especially those affecting individuals' financial status, can be explained and justified.
- ? Trust: Builds trust among users and stakeholders by demonstrating that the AI decisions are transparent and justifiable.

Other options, such as credential theft, prompt injections, and social engineering, are significant concerns but do not directly address the privacy and fairness implications of automated decision-making.

References:

- ? CompTIA SecurityX Study Guide
- ? "The Importance of Explainability in AI," IEEE Xplore
- ? GDPR Article 22, "Automated Individual Decision-Making, Including Profiling"

NEW QUESTION 34

An incident response team is analyzing malware and observes the following:

- Does not execute in a sandbox
- No network IoCs
- No publicly known hash match
- No process injection method detected

Which of the following should the team do next to proceed with further analysis?

- A. Use an online vims analysis tool to analyze the sample
- B. Check for an anti-virtualization code in the sample
- C. Utilize a new deployed machine to run the sample.
- D. Search oilier internal sources for a new sample.

Answer: B

Explanation:

Malware that does not execute in a sandbox environment often contains anti-analysis techniques, such as anti-virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection. Checking for anti-virtualization code is a logical next step because:

- ? It helps determine if the malware is designed to evade analysis tools.
- ? Identifying such code can provide insights into the malware's behavior and intent.
- ? This step can also inform further analysis methods, such as running the malware on physical hardware.

References:

- ? CompTIA Security+ Study Guide
- ? SANS Institute, "Malware Analysis Techniques"
- ? "Practical Malware Analysis" by Michael Sikorski and Andrew Honig

NEW QUESTION 38

After an incident occurred, a team reported during the lessons-learned review that the team.

- * Lost important Information for further analysis.
- * Did not utilize the chain of communication
- * Did not follow the right steps for a proper response

Which of the following solutions is the best way to address these findings?

- A. Requesting budget for better forensic tools to Improve technical capabilities for Incident response operations
- B. Building playbooks for different scenarios and performing regular table-top exercises
- C. Requiring professional incident response certifications for each new team member
- D. Publishing the incident response policy and enforcing it as part of the security awareness program

Answer: B

Explanation:

Building playbooks for different scenarios and performing regular table-top exercises directly addresses the issues identified in the lessons-learned review. Here's why:

- ? Lost important information for further analysis: Playbooks outline step-by-step procedures for incident response, ensuring that team members know exactly what to document and how to preserve evidence.
- ? Did not utilize the chain of communication: Playbooks include communication protocols, specifying who to notify and when. Regular table-top exercises reinforce these communication channels, ensuring they are followed during actual incidents.
- ? Did not follow the right steps for a proper response: Playbooks provide a clear sequence of actions to be taken during various types of incidents, helping the team to respond in a structured and effective manner. Regular exercises allow the team to practice these steps, identifying and correcting any deviations from the plan.

Investing in better forensic tools (Option A) or requiring certifications (Option C) are also valuable, but they do not directly address the procedural and communication gaps identified. Publishing and enforcing the incident response policy (Option D) is important but not as practical and hands-on as playbooks and exercises in ensuring the team is prepared.

References:

- ? CompTIA Security+ Study Guide
- ? NIST SP 800-61 Rev. 2, "Computer Security Incident Handling Guide"
- ? SANS Institute, "Incident Handler's Handbook"

NEW QUESTION 42

A security administrator needs to automate alerting. The server generates structured log files that need to be parsed to determine whether an alarm has been triggered Given the following code function:

```
def parse_logs(logfile):  
    with open(logfile) as log_file:  
        parsed_log = json.load(log_file)  
        if parsed_log["error_log"]["system_1"]["InAlarmState"]:
```

Which of the following is most likely the log input that the code will parse?

A)

```
["error_log"  
  ["system_1"  
    ["InAlarmState": True]
```

B)

```
<"error_log"><"system_1"></"InAlarmState"="True"></"system_1"></"error_log">
```

C)

```
error_log:  
  - system_1:  
    InAlarmState: True
```

D)

```
{"error_log": {"system_1": {"InAlarmState": True }}}
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation:

The code function provided in the question seems to be designed to parse JSON formatted logs to check for an alarm state. Option A is a JSON format that matches the structure likely expected by the code. The presence of the "error_log" and "InAlarmState" keys suggests that this is the correct input format. Reference: CompTIA SecurityX Study Guide, Chapter on Log Management and Automation, Section on Parsing Structured Logs.

NEW QUESTION 43

A cloud engineer needs to identify appropriate solutions to:

- Provide secure access to internal and external cloud resources.
- Eliminate split-tunnel traffic flows.
- Enable identity and access management capabilities.

Which of the following solutions are the most appropriate? (Select two).

- A. Federation
- B. Microsegmentation
- C. CASB
- D. PAM
- E. SD-WAN
- F. SASE

Answer: CF

Explanation:

To provide secure access to internal and external cloud resources, eliminate split-tunnel traffic flows, and enable identity and access management capabilities, the most appropriate solutions are CASB (Cloud Access Security Broker) and SASE (Secure Access Service Edge).

Why CASB and SASE?

? CASB (Cloud Access Security Broker):

? SASE (Secure Access Service Edge):

Other options, while useful, do not comprehensively address all the requirements:

? A. Federation: Useful for identity management but does not eliminate split-tunnel traffic or provide comprehensive security.

? B. Microsegmentation: Enhances security within the network but does not directly address secure access to cloud resources or split-tunnel traffic.

? D. PAM (Privileged Access Management): Focuses on managing privileged accounts and does not provide comprehensive access control for internal and external resources.

? E. SD-WAN: Enhances WAN performance but does not inherently provide the identity and access management capabilities or eliminate split-tunnel traffic.

References:

? CompTIA SecurityX Study Guide

? "CASB: Cloud Access Security Broker," Gartner Research

NEW QUESTION 47

After remote desktop capabilities were deployed in the environment, various vulnerabilities were noticed.

- Exfiltration of intellectual property
- Unencrypted files
- Weak user passwords

Which of the following is the best way to mitigate these vulnerabilities? (Select two).

- A. Implementing data loss prevention
- B. Deploying file integrity monitoring
- C. Restricting access to critical file services only
- D. Deploying directory-based group policies
- E. Enabling modern authentication that supports MFA
- F. Implementing a version control system
- G. Implementing a CMDB platform

Answer: AE

Explanation:

To mitigate the identified vulnerabilities, the following solutions are most appropriate:

? A. Implementing data loss prevention (DLP): DLP solutions help prevent the unauthorized transfer of data outside the organization. This directly addresses the exfiltration of intellectual property by monitoring, detecting, and blocking sensitive data transfers.

? E. Enabling modern authentication that supports Multi-Factor Authentication

(MFA): This significantly enhances security by requiring additional verification methods beyond just passwords. It addresses the issue of weak user passwords by making it much harder for unauthorized users to gain access, even if they obtain the password.

Other options, while useful in specific contexts, do not address all the vulnerabilities mentioned:

? B. Deploying file integrity monitoring helps detect changes to files but does not prevent data exfiltration or address weak passwords.

? C. Restricting access to critical file services improves security but is not comprehensive enough to mitigate all identified vulnerabilities.

? D. Deploying directory-based group policies can enforce security policies but might not directly prevent data exfiltration or ensure strong authentication.

? F. Implementing a version control system helps manage changes to files but is not a security measure for preventing the identified vulnerabilities.

? G. Implementing a CMDB platform (Configuration Management Database) helps manage IT assets but does not address the specific security issues mentioned.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations"

? CIS Controls, "Control 13: Data Protection" and "Control 16: Account Monitoring and Control"

NEW QUESTION 50

SIMULATION

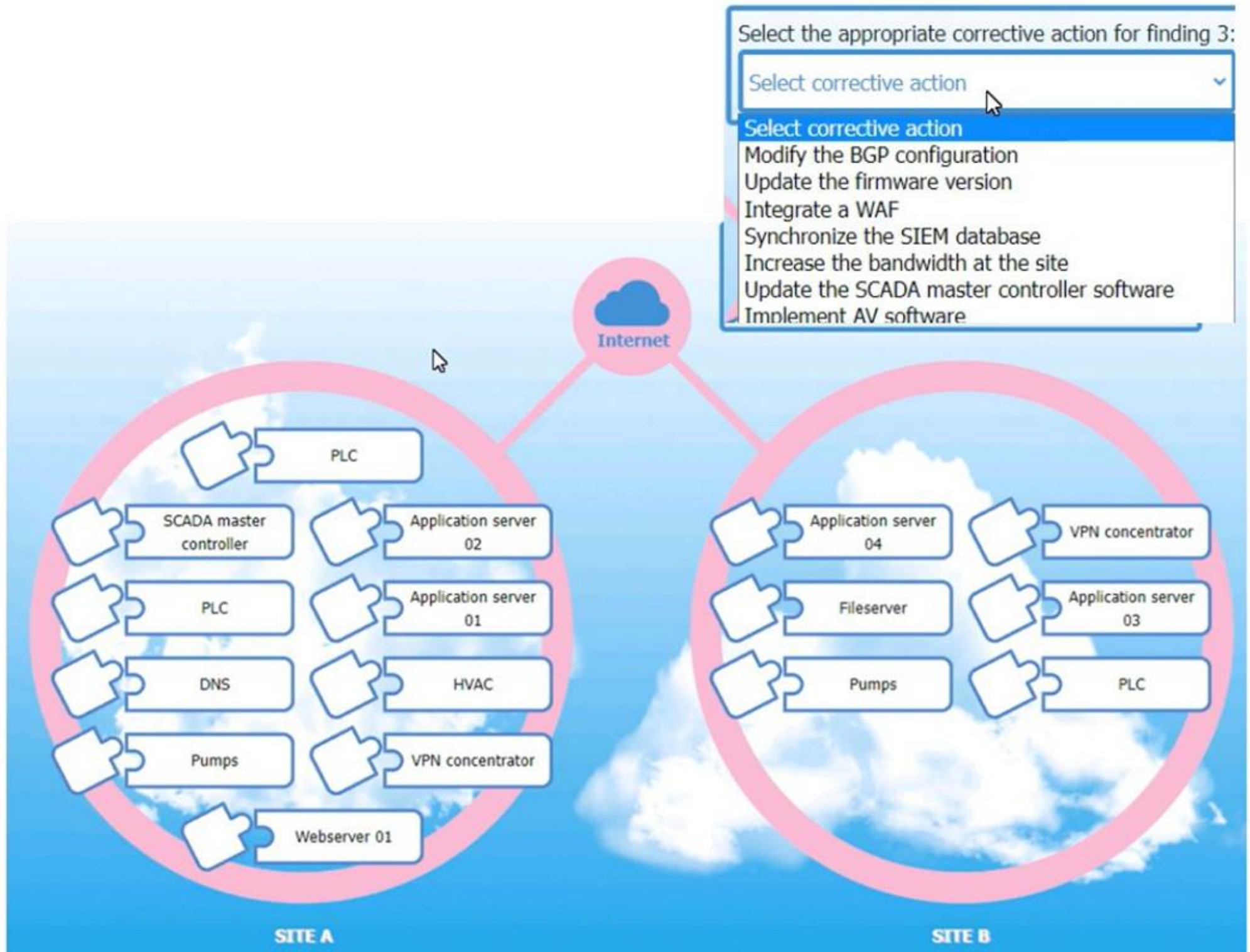
An organization is planning for disaster recovery and continuity of operations, and has noted the following relevant findings:

- * 1. A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.
- * 2. A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.
- * 3. A natural disaster may disrupt operations at Site A, which would then cause unreliable internet connectivity at Site B due to route flapping.

INSTRUCTIONS

Match each relevant finding to the affected host by clicking on the host name and selecting the appropriate number.

For findings 1 and 2, select the items that should be replicated to Site B. For finding 3, select the item requiring configuration changes, then select the appropriate corrective action from the drop-down menu.



Relevant findings
✕

1

A natural disaster may disrupt operations at Site A, which would then cause an evacuation. Users are unable to log into the domain from their workstations after relocating to Site B.

Select this for the item that should be replicated to Site B.

2

A natural disaster may disrupt operations at Site A, which would then cause the pump room at Site B to become inoperable.

Select this for the item that should be replicated to Site B.

3

A natural disaster may disrupt operations at Site A, which would then cause unreliable Internet connectivity at Site B due to route flapping.

Select this for the item requiring configuration changes.

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Matching Relevant Findings to the Affected Hosts:

? Finding 1:

? Finding 2:

? Finding 3:

Corrective Actions for Finding 3:

? Finding 3 Corrective Action:

? Replication to Site B for Finding 1:

? Replication to Site B for Finding 2:

? Configuration Changes for Finding 3:

References:

? CompTIA Security+ Study Guide: This guide provides detailed information on disaster recovery and continuity of operations, emphasizing the importance of replicating critical services and making necessary configuration changes to ensure seamless operation during disruptions.

? CompTIA Security+ Exam Objectives: These objectives highlight key areas in disaster recovery planning, including the replication of critical services and network configuration adjustments.

? Disaster Recovery and Business Continuity Planning (DRBCP): This resource outlines best practices for ensuring that operations can continue at an alternate site during a disaster, including the replication of essential services and network stability measures.

By ensuring that critical services like DNS and control systems for pumps are replicated at the alternate site, and by addressing network routing issues through proper BGP configuration, the organization can maintain operational continuity and minimize the impact of natural disasters on their operations.

NEW QUESTION 54

Asecuntv administrator is performing a gap assessment against a specific OS benchmark The benchmark requires the following configurations be applied to endpoints:

- Full disk encryption
- * Host-based firewall
- Time synchronization
- * Password policies
- Application allow listing
- * Zero Trust application access

Which of the following solutions best addresses the requirements? (Select two).

- A. CASB
 B. SBoM
 C. SCAP
 D. SASE
 E. HIDS

Answer: CD

Explanation:

To address the specific OS benchmark configurations, the following solutions are most appropriate:

* C. SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies.

* D. SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant

access to applications and data.

These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.

References:

? CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures.

? NIST Special Publication 800-126, "The Technical Specification for the Security Content Automation Protocol (SCAP)": Details SCAP's role in security automation.

? "Zero Trust Networks: Building Secure Systems in Untrusted Networks" by Evan Gilman and Doug Barth: Covers the principles of Zero Trust and how SASE can implement them.

By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintained effectively.

NEW QUESTION 58

A software development team requires valid data for internal tests. Company regulations, however do not allow the use of this data in cleartext. Which of the following solutions best meet these requirements?

- A. Configuring data hashing
- B. Deploying tokenization
- C. Replacing data with null record
- D. Implementing data obfuscation

Answer: B

Explanation:

Tokenization replaces sensitive data elements with non-sensitive equivalents, called tokens, that can be used within the internal tests. The original data is stored securely and can be retrieved if necessary. This approach allows the software development team to work with data that appears realistic and valid without exposing the actual sensitive information.

Configuring data hashing (Option A) is not suitable for test data as it transforms the data into a fixed-length value that is not usable in the same way as the original data. Replacing

data with null records (Option C) is not useful as it does not provide valid data for testing. Data obfuscation (Option D) could be an alternative but might not meet the regulatory requirements as effectively as tokenization.

References:

? CompTIA Security+ Study Guide

? NIST SP 800-57 Part 1 Rev. 5, "Recommendation for Key Management"

? PCI DSS Tokenization Guidelines

NEW QUESTION 59

A systems administrator wants to reduce the number of failed patch deployments in an organization. The administrator discovers that system owners modify systems or applications in an ad hoc manner. Which of the following is the best way to reduce the number of failed patch deployments?

- A. Compliance tracking
- B. Situational awareness
- C. Change management
- D. Quality assurance

Answer: C

Explanation:

To reduce the number of failed patch deployments, the systems administrator should implement a robust change management process. Change management ensures that all modifications to systems or applications are planned, tested, and approved before deployment. This systematic approach reduces the risk of unplanned changes that can cause patch failures and ensures that patches are deployed in a controlled and predictable manner.

References:

? CompTIA SecurityX Study Guide: Emphasizes the importance of change management in maintaining system integrity and ensuring successful patch deployments.

? ITIL (Information Technology Infrastructure Library) Framework: Provides best practices for change management in IT services.

? "The Phoenix Project" by Gene Kim, Kevin Behr, and George Spafford: Discusses the critical role of change management in IT operations and its impact on system stability and reliability.

NEW QUESTION 61

A network engineer must ensure that always-on VPN access is enabled Curt restricted to company assets Which of the following best describes what the engineer needs to do"

- A. Generate device certificates using the specific template settings needed
- B. Modify signing certificates in order to support IKE version 2
- C. Create a wildcard certificate for connections from public networks
- D. Add the VPN hostname as a SAN entry on the root certificate

Answer: A

Explanation:

To ensure always-on VPN access is enabled and restricted to company assets, the network engineer needs to generate device certificates using the specific template settings required for the company's VPN solution. These certificates ensure that only authorized devices can establish a VPN connection.

Why Device Certificates are Necessary:

? Authentication: Device certificates authenticate company assets, ensuring that only authorized devices can access the VPN.

? Security: Certificates provide a higher level of security compared to username and password combinations, reducing the risk of unauthorized access.

? Compliance: Certificates help in meeting security policies and compliance requirements by ensuring that only managed devices can connect to the corporate network.

Other options do not provide the same level of control and security for always-on VPN access:

? B. Modify signing certificates for IKE version 2: While important for VPN protocols, it does not address device-specific authentication.

? C. Create a wildcard certificate: This is not suitable for device-specific authentication and could introduce security risks.

? D. Add the VPN hostname as a SAN entry: This is more related to certificate management and does not ensure device-specific authentication.

References:

- ? CompTIA SecurityX Study Guide
- ? "Device Certificates for VPN Access," Cisco Documentation
- ? NIST Special Publication 800-77, "Guide to IPsec VPNs"

NEW QUESTION 63

A security engineer needs to secure the OT environment based on the following requirements

- Isolate the OT network segment
- Restrict Internet access.
- Apply security updates to workstations
- Provide remote access to third-party vendors

Which of the following design strategies should the engineer implement to best meet these requirements?

- A. Deploy a jump box on the third party network to access the OT environment and provide updates using a physical delivery method on the workstations
- B. Implement a bastion host in the OT network with security tools in place to monitor access and use a dedicated update server for the workstations.
- C. Enable outbound internet access on the OT firewall to any destination IP address and use the centralized update server for the workstations
- D. Create a staging environment on the OT network for the third-party vendor to access and enable automatic updates on the workstations.

Answer: B

Explanation:

To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host in the OT network. The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.

References:

- ? CompTIA SecurityX Study Guide: Recommends the use of bastion hosts and dedicated update servers for securing OT environments.
- ? NIST Special Publication 800-82, "Guide to Industrial Control Systems (ICS) Security": Advises on isolating OT networks and using secure remote access methods.
- ? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill: Discusses strategies for securing OT networks, including the use of bastion hosts and update servers.

NEW QUESTION 66

A software engineer is creating a CI/CD pipeline to support the development of a web application. The DevSecOps team is required to identify syntax errors. Which of the following is the most relevant to the DevSecOps team's task?

- A. Static application security testing
- B. Software composition analysis
- C. Runtime application self-protection
- D. Web application vulnerability scanning

Answer: A

Explanation:

Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security issues early in the development lifecycle.

- ? A. Static application security testing (SAST): SAST tools analyze the source code to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.
- ? B. Software composition analysis: This focuses on identifying vulnerabilities in open-source components and libraries used in the application but does not address syntax errors directly.
- ? C. Runtime application self-protection (RASP): RASP involves monitoring and protecting applications during runtime, which does not help in identifying syntax errors during the development phase.
- ? D. Web application vulnerability scanning: This involves scanning the running application for vulnerabilities but does not address syntax errors in the code.

References:

- ? CompTIA Security+ Study Guide
- ? OWASP (Open Web Application Security Project) guidelines on SAST
- ? NIST SP 800-95, "Guide to Secure Web Services" Top of Form
Bottom of Form

NEW QUESTION 71

A company isolated its OT systems from other areas of the corporate network. These systems are required to report usage information over the internet to the vendor. Which of the following best reduces the risk of compromise or sabotage? (Select two).

- A. Implementing allow lists
- B. Monitoring network behavior
- C. Encrypting data at rest
- D. Performing boot integrity checks
- E. Executing daily health checks
- F. Implementing a site-to-site IPsec VPN

Answer: AF

Explanation:

- ? A. Implementing allow lists: Allow lists (whitelisting) restrict network communication to only authorized devices and applications, significantly reducing the attack surface by ensuring that only pre-approved traffic is permitted.
 - ? F. Implementing a site-to-site IPsec VPN: A site-to-site VPN provides a secure, encrypted tunnel for data transmission between the OT systems and the vendor, protecting the data from interception and tampering during transit.
- Other options:

- ? B. Monitoring network behavior: While useful for detecting anomalies, it does not proactively reduce the risk of compromise or sabotage.
- ? C. Encrypting data at rest: Important for protecting data stored on devices, but does not address network communication risks.
- ? D. Performing boot integrity checks: Ensures the integrity of the system at startup but does not protect ongoing network communications.
- ? E. Executing daily health checks: Useful for maintaining system health but does not directly reduce the risk of network-based compromise or sabotage.

References:

- ? CompTIA Security+ Study Guide
- ? NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security"
- ? "Industrial Network Security" by Eric D. Knapp and Joel Thomas Langill

NEW QUESTION 75

A software company deployed a new application based on its internal code repository. Several customers are reporting anti-malware alerts on workstations used to test the application. Which of the following is the most likely cause of the alerts?

- A. Misconfigured code commit
- B. Unsecure bundled libraries
- C. Invalid code signing certificate
- D. Data leakage

Answer: B

Explanation:

The most likely cause of the anti-malware alerts on customer workstations is unsecure bundled libraries. When developing and deploying new applications, it is common for developers to use third-party libraries. If these libraries are not properly vetted for security, they can introduce vulnerabilities or malicious code.

Why Unsecure Bundled Libraries?

- ? Third-Party Risks: Using libraries that are not secure can lead to malware infections if the libraries contain malicious code or vulnerabilities.
- ? Code Dependencies: Libraries may have dependencies that are not secure, leading to potential security risks.
- ? Common Issue: This is a frequent issue in software development where libraries are used for convenience but not properly vetted for security.

Other options, while relevant, are less likely to cause widespread anti-malware alerts:

- ? A. Misconfigured code commit: Could lead to issues but less likely to trigger anti-malware alerts.
- ? C. Invalid code signing certificate: Would lead to trust issues but not typically anti-malware alerts.
- ? D. Data leakage: Relevant for privacy concerns but not directly related to anti-malware alerts.

References:

- ? CompTIA SecurityX Study Guide
- ? "Securing Open Source Libraries," OWASP
- ? "Managing Third-Party Software Security Risks," Gartner Research

NEW QUESTION 76

A security architect is establishing requirements to design resilience in an enterprise system. The system must be extended to other physical locations. The system must

- Be survivable to one environmental catastrophe
- Be recoverable within 24 hours of critical loss of availability
- Be resilient to active exploitation of one site-to-site VPN solution

- A. Load-balance connection attempts and data ingress at internet gateways
- B. Allocate fully redundant and geographically distributed standby sites.
- C. Employ layering of routers from diverse vendors
- D. Lease space to establish cold sites throughout other countries
- E. Use orchestration to procure, provision, and transfer application workloads to cloud services
- F. Implement full weekly backups to be stored off-site for each of the company's sites

Answer: B

Explanation:

To design resilience in an enterprise system that can survive environmental catastrophes, recover within 24 hours, and be resilient to active exploitation, the best strategy is to allocate fully redundant and geographically distributed standby sites. Here's why:

- ? Geographical Redundancy: Having geographically distributed standby sites ensures that if one site is affected by an environmental catastrophe, the other sites can take over, providing continuity of operations.
- ? Full Redundancy: Fully redundant sites mean that all critical systems and data are replicated, enabling quick recovery in the event of a critical loss of availability.
- ? Resilience to Exploitation: Distributing resources across multiple sites reduces the risk of a single point of failure and increases resilience against targeted attacks.

? References:

NEW QUESTION 77

SIMULATION

During the course of normal SOC operations, three anomalous events occurred and were flagged as potential IoCs. Evidence for each of these potential IoCs is provided.

INSTRUCTIONS

Review each of the events and select the appropriate analysis and remediation options for each IoC.

IoC 1		IoC 2		IoC 3	
Source	Svc	Type	Dest	Data	
Apache_httpd		DNSQ	@10.1.1.1:53	update.s.domain	
Apache_httpd		DNSQR	@10.1.2.5	CNAME 3a129sk219r0slsmfkzzz000.s.domain	
Apache_httpd		DNSQ	@10.1.1.1:53	3a129sk219r0slsmfkzzz000.s.domain	
Apache_httpd		DNSQR	@10.1.2.5	IN A 108.158.253.253	

Select analysis

- An employee is attempting to access a blocked website.
- Someone is footprinting a network subnet.
- A host is participating in an IRC-based botnet.
- Service identification and fingerprinting are occurring.
- Canonical name records in a public DNS cache are being updated.
- An application is performing an automatic update.
- An employee is using P2P services to download files.
- The service is attempting to resolve a malicious domain.

Select analysis

Select remediation

- Enforce endpoint controls on third-party software installations.
- Investigate for software supply-chain attacks.
- Configure the DNS server to perform recursion.
- Block ping requests across the WAN interface.
- Deploy a network-based DLP solution.
- Implement a blocklist for known malicious ports.
- No further action is needed.

Select remediation

IoC 1		IoC 2		IoC 3	
Src	Dst	Proto	Data	Action	
10.0.5.5	10.1.2.1	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.2	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.3	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.4	IP_ICMP	ECHO	Drop	
10.0.5.5	10.1.2.5	IP_ICMP	ECHO	Drop	

Select analysis

- An employee is attempting to access a blocked website.
- Someone is footprinting a network subnet.
- A host is participating in an IRC-based botnet.
- Service identification and fingerprinting are occurring.
- Canonical name records in a public DNS cache are being updated.
- An application is performing an automatic update.
- An employee is using P2P services to download files.
- The service is attempting to resolve a malicious domain.

Select analysis

Select remediation

- Enforce endpoint controls on third-party software installations.
- Investigate for software supply-chain attacks.
- Configure the DNS server to perform recursion.
- Block ping requests across the WAN interface.
- Deploy a network-based DLP solution.
- Implement a blocklist for known malicious ports.
- No further action is needed.

Select remediation

IoC 1

IoC 2

IoC 3

Proxylog>
> GET /announce?info_hash=%01d%FE%7E%F1%10%5CwvAp%ED%F6%03%C49%D6B%14%F1&
> peer_id=%B8js%7F%E8%0C%AFh%02Y%967%24e%27V%EEM%16%5B&port=41730&
> uploaded=0&downloaded=0&left=3767869&compact=1&ip=10.5.1.26&event=started
> HTTP/1.1
> Accept: application/x-bittorrent
> Accept-Encoding: gzip
> User-Agent: RAZA 2.1.0.0
> Host: localhost
> Connection: Keep-Alive
<
< HTTP 200 OK

Select analysis

An employee is attempting to access a blocked website.
Someone is footprinting a network subnet.
A host is participating in an IRC-based botnet.
Service identification and fingerprinting are occurring.
Canonical name records in a public DNS cache are being updated.
An application is performing an automatic update.
An employee is using P2P services to download files.
The service is attempting to resolve a malicious domain.

Select analysis

Remediation

Select remediation

Enforce endpoint controls on third-party software installations.
Investigate for software supply-chain attacks.
Configure the DNS server to perform recursion.
Block ping requests across the WAN interface.
Deploy a network-based DLP solution.
Implement a blocklist for known malicious ports.
No further action is needed.

Select remediation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Analysis and Remediation Options for Each IoC: IoC 1:

? Evidence:

? Analysis:

? Remediation:

IoC 2:

? Evidence:

? Analysis:

? Remediation:

IoC 3:

? Evidence:

? Analysis:

? Remediation:

References:

? CompTIA Security+ Study Guide: This guide offers detailed explanations on identifying and mitigating various types of Indicators of Compromise (IoCs) and the corresponding analysis and remediation strategies.

? CompTIA Security+ Exam Objectives: These objectives cover key concepts in network security monitoring and incident response, providing guidelines on how to handle different types of security events.

? Security Operations Center (SOC) Best Practices: This resource outlines effective strategies for analyzing and responding to anomalous events within a SOC, including the use of blocklists, endpoint controls, and network configuration changes.

By accurately analyzing the nature of each IoC and applying the appropriate remediation measures, the organization can effectively mitigate potential security threats and maintain a robust security posture.

NEW QUESTION 79

A security analyst received a report that an internal web page is down after a company- wide update to the web browser Given the following error message:

Your connection is not private.

Attackers might be trying to steal your information for www.internalwebsite.company.com.

NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM

Which of the following is the best way to fix this issue?

- A. Rewriting any legacy web functions
- B. Disabling all deprecated ciphers

- C. Blocking all non-essential ports
- D. Discontinuing the use of self-signed certificates

Answer: D

Explanation:

The error message "NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM" indicates that the web browser is rejecting the certificate because it uses a weak signature algorithm. This commonly happens with self-signed certificates, which often use outdated or insecure algorithms.

Why Discontinue Self-Signed Certificates?

? Security Compliance: Modern browsers enforce strict security standards and may reject certificates that do not comply with these standards.

? Trusted Certificates: Using certificates from a trusted Certificate Authority (CA) ensures compliance with security standards and is less likely to be flagged as insecure.

? Weak Signature Algorithm: Self-signed certificates might use weak algorithms like MD5 or SHA-1, which are considered insecure.

Other options do not address the specific cause of the certificate error:

? A. Rewriting legacy web functions: Does not address the certificate issue.

? B. Disabling deprecated ciphers: Useful for improving security but not related to the certificate error.

? C. Blocking non-essential ports: This is unrelated to the issue of certificate validation.

References:

? CompTIA SecurityX Study Guide

? "Managing SSL/TLS Certificates," OWASP

? "Best Practices for Certificate Management," NIST Special Publication 800-57

NEW QUESTION 84

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

CAS-005 Practice Exam Features:

- * CAS-005 Questions and Answers Updated Frequently
- * CAS-005 Practice Questions Verified by Expert Senior Certified Staff
- * CAS-005 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CAS-005 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CAS-005 Practice Test Here](#)